

Exhibit 2

SENATE COMMITTEE ON JUDICIARY
Bill Lockyer, Chairman
1987-88 Regular Session

SB 255 (Davis)
As introduced
Penal Code
TDT

S
B

2
5
5

COMPUTER CRIME

HISTORY

Source: Los Angeles County Board of Supervisors

Prior Legislation: SB 1786 (1986) - Died in
Assembly Judiciary
AB 2551 (1983) - Chaptered

Support: Union Bank, Security Pacific National
Bank, Information Systems Security
Association, Southern California Gas
Company, California Bankers
Association, Hughes Aircraft, Santa
Cruz County Board of Supervisors,
Northrop Corporation, Los Angeles
County Sheriff, Attorney General,
Equifax Inc., Los Angeles County
District Attorney

Opposition: No known

KEY ISSUE

SHOULD A COMPREHENSIVE COMPUTER DATA ACCESS AND
FRAUD ACT BE ADOPTED WHICH WOULD REDEFINE A NUMBER
OF COMPUTER TERMS, ESTABLISH SEVEN SPECIFIC
CRIMES, PROVIDE FOR COMPENSATORY DAMAGES AS CIVIL
REMEDIES AND PERMIT SEIZURE OF PRIVATE COMPUTER
EQUIPMENT?

LEGISLATIVE INTENT SERVICE (800) 666-1917



(More)

SB 255 (Davis)
Page 2

PURPOSE

Existing law makes it a crime, punishable by imprisonment and fines which in no case may exceed \$10,000, for any person to, among other things, access a computer system or network: 1) intentionally in order to defraud or extort; 2) maliciously; or 3) intentionally and without authorization, with the knowledge that the access was unauthorized.

This bill would repeal and then rewrite Penal Code Section 502. It would broaden existing definitions, expand the scope of prohibited computer related activity, and restructure fines and imprisonment penalties for violations.

It would reenact civil remedy provisions and add a new penalty of seizure of computer equipment used in committing violations of the act. Finally, it would set forth the legislative intent of this bill.

The purpose of the bill is to clarify and broaden existing law, as well as provide increased penalties commensurate with the gravity of the offense.

COMMENT

1. Background

This bill was developed by the Computer Crime Task Force, which is a subcommittee of the Los Angeles County Criminal Justice Coordinating Committee. The Task Force is composed of 16 members including representatives from law enforcement, district attorney offices, the

(More)



SB 255 (Davis)
Page 3

U.S. Attorney's office, and private industry, including banks, accounting firms and big business. No representatives of the defense bar are on the Task Force. The primary duty of the task force is to develop a Model Computer Crime Act; and, in so doing, it created a bill which it believes would meet the specific computer crime problems in California.

2. Standardization of definitions

This bill would broaden the application of existing law by redefining terms that are used in existing law, such as "access", "computer system", "computer network", "computer program" and "data". It would also define new terms, such as "computer services" and "supporting documentation".

The task force believes that it is necessary to provide standard definitions in order to insure higher conviction rates. Proponents believe that the new definitions would be broader, and would be directed more to computer users than lawyers but would be acceptable to both the business and legal communities.

3. New crimes

This bill would create seven new crimes involving computers. Any person who did any of the following acts, if the act was not within the course and scope of employment, would be guilty of a crime:

(More)



SB 255 (Davis)
Page 4

- a) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud or deceive, or (B) wrongfully control or obtain money, property, data, or services.
- b) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
- c) Knowingly and without permission uses or causes to be used computer services.
- d) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
- e) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
- f) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or

(More)

(800) 666-1917

LEGISLATIVE INTENT SERVICE



SB 255 (Davis)
Page 5

computer network in violation of this section.

- g) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

4. Penalties

Existing penalties for maliciously or intentionally accessing a computer system or network in order to defraud or extort is punishable by imprisonment and a fine which in no case may exceed \$10,000. Intentionally accessing a computer system or network without authorization when no injury results, is an infraction punishable by a fine not exceeding \$250. If injury results, or if it is a second offense, the fine could be imposed not to exceed \$5,000 and/or imprisonment in county jail not exceeding one year.

This bill would increase the penalties as follows:

a. Access (Hacking)

- 1) A first offense or an offense where no injury occurs would remain an infraction punishable by a fine of up to \$250.
- 2) Repeated access or access resulting in injury would be punishable as a wobbler, by a fine of \$10,000 maximum or imprisonment in state prison for 16 months or 2 or 3 years or both, or a fine of \$5,000 maximum or 1 year in county jail or both.

(More)



SB 255 (Davis)
Page 6

b. Unauthorized use of computer services

- 1) A first offense without injury where the value of services used is \$400 or less, would be punishable by a fine of up to \$5,000 or one year in county jail or both.
- 2) Subsequent offenses or violations causing injury would be subject to the same felony/misdemeanor punishment as repeat access or access with injury.

c. Remaining computer crimes

All the remaining computer crimes including altering, data theft, tampering with systems, publishing access codes, disrupting, or committing fraud or theft via computer, whether a first or subsequent offense, would be subject to the same felony/misdemeanor punishment as repeat access or access with injury.

5. Civil penalties

In addition to any other available civil remedies, the owner or lessee of the computer would be permitted to bring a civil action against any person convicted of any of the enumerated crimes for compensatory damages. Actions of an unemancipated minor would be imputed to the parent or legal guardian having control or custody of the minor. The court would be authorized to award reasonable attorney's fees to a prevailing party.

(More)



SB 255 (Davis)
Page 7

6. Intent not required

Under existing law, the criminal conduct must be "intentional" or "malicious". This bill would establish a new standard that the conduct be "knowingly and without permission". Proponents claim that this new standard would make these crimes "general intent" crimes, which would be easier for the public to understand and authorities to enforce.

One effect of this change would be to make such acts as unintentional and inadvertent alteration of data by an employee using a computer for a personal project without permission, subject to a state prison term.

7. Felony penalty for first time access

Under this bill, unauthorized access which caused injury would be punishable as a felony or misdemeanor. Because injury is so broadly defined, all first time hackers could be found guilty of a felony.

8. Injury broadly defined

Injury is defined to include not only damage or destruction to the computer and its data but also "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system...or data was or was not altered, deleted, damaged or destroyed by the access." Thus, the fact that a computer owner incurs some costs to insure that a computer was not altered would trigger a state prison felony penalty even if the offense involved was first time access by a

(More)

(800) 666-1917

LEGISLATIVE INTENT SERVICE



SB 255 (Davis)

Page 8

hacker. Arguably such verification would be necessary whenever unauthorized access occurs, thus every first offense without damage could be a felony.

9. Employee misuse

Under this bill, an employee who used a computer more than once for such personal projects as preparing a personal letter, maintaining a mailing list or recipe list, accessing computer data to use in a term paper, or sending computer messages to other employees, could be guilty of a felony, even if the use occurred after work and caused no injury. On the other hand, an employee who uses the employer's computer system or data within the scope of employment would not be violating the statute.

10. Confiscation of property

This bill would authorize law enforcement officers to seize, under warrant or without warrant incident to a lawful arrest, any computer, computer system, computer program, instrument, apparatus, device, plans, instruction, or written publication used in the commission of any crime established under this Act. After conviction and a hearing to determine property rights, the seized computer equipment, if owned or controlled by the person so convicted, or owned or controlled by a person or entity that knowingly allowed the use of the seized item in the commission of any computer crime prohibited by this bill, could be destroyed as contraband by the sheriff of the county in which the person was

(More)



SB 255 (Davis)
Page 9

convicted, or given to the county for its use or for donation to any other public entity or nonprofit corporation.

This provision of the bill would allow confiscation and destruction of a costly computer system owned by another as a penalty for a first time access which caused no injury and which may be disposed of as an infraction or misdemeanor.

It could be argued that the seizure of computers used for these offenses might unjustly affect other innocent persons who have a property interest in these computers.

